



微隔离（龙侍）

产品文档





文档目录

产品简介

功能概述

简介

相关概念

相关服务

使用微隔离产品

功能和优势

可靠

安全

易用

工作组

工作组概述

什么是工作组

什么是资产标签

工作组使用简介

安全策略

安全策略概述

什么是安全策略

安全策略设置思路

策略使用简介

快速入门

步骤一：工作组管理

步骤二：标签管理

步骤三：负载管理

步骤四：角色标签

步骤五：安全策略

步骤六：安全告警

最佳实践

工作组



产品简介

功能概述

简介

最近更新时间: 2023-02-10 10:00:31

微隔离(龙侍)为用户提供基于主机的网络访问策略配置服务，通过主机层的实时监控，帮助用户发现系统中的异常访问情况，并通过对应的阻断策略和隔离方式，帮助用户从主机层实现系统中网络的微隔离管理。

用户在其管理端对其所管理的主机资产进行分组和标签设置，并根据这些配置设置对应的安全策略。通过这些策略，用户可以设置资产的访问白名单，当有非白名单访问关系出现的时候，可以产生告警，并设置对应的自动隔离策略。

如果用户的系统中，发现了一台被沦陷的主机（威胁情报、入侵检测告警、访问异常告警等信息），用户可以选择一键隔离该主机，这样该主机就无法对外进行访问，将已经发生的风险限制在一个可控范围内。

总结来说，微隔离产品通过基于主机的网络访问实时监控和服务端的策略管理，实现了用户在主机侧对东西流量的监控和异常行为的处理，实时保障用户的重点资产并及时隔离用户的陷落主机，保障用户的云安全。



相关概念

最近更新时间: 2023-02-10 10:00:31

了解微隔离时，通常会涉及到以下概念：

- **微隔离**：Micro - Segmentation，微隔离，也叫微分段。从产品的使用来说，其实应该是先做分段，再做隔离。也就是先将用户访问关系设置好对应的规则，然后对不符合规则的行为进行告警。其实这个理念同时也和零信任是天然吻合的，所以在很多讲零信任的产品里，也会提到这个概念。
- **访问策略**：配置访问策略，来监控主机之间的访问情况，对于不符合访问策略的信息，进行告警或放行等相关处置。
- **单资产隔离**：当单个资产受到攻击或者产生异常对外访问的时候，可以进行单资产隔离。隔离后，资产可以和安全后台进行通信，但是无法访问其他机器。
- **资产标签**：根据每个资产的业务属性，设置其标签。
- **工作组**：根据资产的业务属性，将资产聚合成工作组。



相关服务

最近更新时间: 2023-02-10 10:00:31

- 您可以对具有相同业务特点或者服务特点的机器配置为工作组。
- 您可以对工作组和工作组之间的访问关系设置访问策略。
- 根据策略，系统会监控访问组之间的访问关系，您可以查看告警结果。
- 您可以根据告警和其他相关信息，对特定资产进行单资产隔离。



使用微隔离产品

最近更新时间: 2023-02-10 10:00:31

微隔离提供基于Web的租户端用户界面，即控制台，如果您已注册云平台账户并开通了微隔离功能，您可以直接登录控制台，跳转到微隔离界面使用相关功能。

微隔离也提供了 API 接口方便您通过 API 接口查询相关信息。



功能和优势

可靠

最近更新时间: 2023-02-10 15:50:23

致力于打造业界最为可靠的微隔离服务。

- 低资源占用：一键部署轻量级Agent，高性能、低占用CPU/内存，兼容多个主流操作系统。
- 高稳定性架构：客户端具备bypass机制，确保各类异常场景均不影响业务流量通行。



安全

最近更新时间: 2023-02-10 15:50:23

微隔离通过自己的设计方式，提供安全的服务能力。

- 访问控制：不同租户之间的访问隔离。
- 双向认证：在客户端和服务端之间提供双向认证。



易用

最近更新时间: 2023-02-10 15:50:23

提供易用的微隔离服务管理和使用方法。

- 将安全控制与资产配置在一起。
- 充当天线（遥测）并收集有关工作负载的信息，然后将这些信息用于微分段策略和执行。
- 利用现有的基于主机的安全功能（即基于主机的防火墙和网络过滤）。
- 与移动和临时工作负载匹配良好。



工作组

工作组概述

什么是工作组

最近更新时间: 2023-02-10 15:55:18

工作组可理解为根据资产的业务、服务或者其他属性，进行合并的一个组。

微隔离会通过为工作组之间的访问关系，设置访问策略，监控其访问数据，并产生和规则对应的告警，同时提供相关处置能力。



什么是资产标签

最近更新时间: 2023-02-10 15:55:18

资产标签包括以下几个维度。

- 业务维度：业务维度指的是根据资产提供的业务服务，例如记账的业务，客户信息的业务等。根据业务维度进行分组，是考虑到业务之间有固定的访问逻辑，在后续制定策略的时候可以通过业务维度标签快速进行设置。
- 环境维度：根据部署和工作的需要，一般会有包括工作环境、测试环境、正式环境等，而环境和环境之间的访问关系一般也有对应的要求。策略制定的时候可以通过环境维度，设置访问策略。
- 位置维度：位置维度包括了资产部署的地理位置或者是所属的云体系，不同位置维度之间有对应的访问逻辑，可以根据这个进行测量设置。



工作组使用简介

最近更新时间: 2023-02-10 15:50:23

工作组的作用是通过几个维度的标签给资产进行配置。然后，并根据资产的特性，将这些资产进行分组。例如，将属于相同业务和环境的资产放到相同的组，然后根据这些组的访问关系，在策略里设置对应的访问策略，从而监控相关的访问情况。



安全策略

安全策略概述

什么是安全策略

最近更新时间: 2023-02-10 15:55:18

安全策略是通过设置组和组之间的访问关系，从而可以通过监控组与组之间的访问关系，如果出现访问关系和设置的安全策略不符合，就会产生告警。



安全策略设置思路

最近更新时间: 2023-02-10 15:55:18

安全策略的设置思路来自于以下几点： 1) 根据当前的业务访问情况，对有固定访问逻辑的工作组之间设置访问关系。 2) 当访问关系发生变化的时候，调整访问关系。 3) 如果触发了安全策略的告警，根据业务情况和安全整体信息，选择优化安全策略或者隔离对应的资产。



策略使用简介

最近更新时间: 2023-02-10 15:50:23

策略的使用包括两个方面

- 1) 根据业务工作情况，设置对应的安全策略。
- 2) 如果有触发策略信息的告警，根据实际情况进行排查，然后进行安全策略优化或者进行隔离设置。



快速入门

步骤一：工作组管理

最近更新时间: 2023-02-10 16:12:39

微隔离服务

资产管理

工作组

工作负载

安全策略管理

安全事件

工作组

标签

工作组总量

7个

分组状态

未关联资产工作组

5个

未关联策略工作组

3个

放行工作组

4个

告警工作组

2个

阻断工作组

1个

新增工作组

多个关键字用竖线 "|" 分隔。多个过滤标签用回车键分隔

工作组名称	关联资产	业务	环境	位置	隔离策略	创建时间	修改时间	操作
比邛	0个	业务poc	-	-	放行	2022-04-20 10:41...	2022-04-20 10:41...	编辑 删除
xx11	0个	业务poc	-	-	放行	2022-04-15 14:53...	2022-04-20 10:13...	编辑 删除
testzhang	0个	业务poc	-	-	放行	2022-04-15 14:51...	2022-04-15 14:51...	编辑 删除
poc	3个	业务poc	环境poc	深圳	告警	2022-04-07 12:51...	2022-04-13 16:46...	编辑 删除
南洋测试工作组	2个	测试业务	生产环境	深圳	告警	2022-04-05 15:10...	2022-04-13 11:14...	编辑 删除
南洋测试组2	0个	测试业务	-	-	阻断	2022-04-05 15:13...	2022-04-13 10:38...	编辑 删除

查看工作组信息

在工作组的页面，用户可以看到以下信息。

- 1) 数据统计。统计包括总共设计的工作组（工作组总量）、分组状态的相关信息（未关联资产工作组、未关联策略工作组、放行工作组、告警工作组、阻断工作组）。
- 2) 工作组的列表信息。以列表形式查看所有的工作组信息。
- 3) 查看和编辑工作组的详细信息。点击【编辑】可以查看并编辑详细的工作组信息。

新建工作组

根据业务情况，用户可以设置新的工作组。



新建工作组

×

组名信息

名称

请输入工作组名称，不超过32个字符

备注

请输入备注信息，不超过128个字符

标签信息

业务

请选择业务标签

环境

请选择环境标签

位置

请选择位置标签

资产信息

选择资产来源

DEFAULT

选择主机节点

已选择 0 个主机节点

清空选择

请输入主机节点名称/IP进行搜索

Q

☐

主机名称/IP

角色标签

暂无数据

主机名称/IP

角色标签

完成

完成并创建策略

取消

新建工作组需要填写的信息说明如下。

- 1) 工作组名称。工作组的具体名称。
- 2) 备注。关于工作组的备注信息。
- 3) 工作组的业务标签、环境标签和位置标签。设置工作组的业务标签、环境标签和位置标签。
- 4) 工作组的具体资产。选择属于该工作组的具体资产信息。



步骤二：标签管理

最近更新时间: 2023-02-10 16:03:42

工作组

工作组 标签

📋

业务标签数

3 ↑

🌐

环境标签数

4 ↑

📍

位置标签数

3 ↑

新增标签

全部标签类型

多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

🔍

🔄

标签名称	标签类型	关联工作组	标签描述	创建时间 ⬆	修改时间 ⬇	操作 ⓘ
abc	环境	0	-	2022-04-07 19:59:03	2022-04-07 19:59:03	编辑 删除
位置poc	位置	0	-	2022-04-07 12:50:22	2022-04-07 12:50:22	编辑 删除
环境poc	环境	1	-	2022-04-07 12:50:01	2022-04-07 12:50:01	编辑 删除
业务poc	业务	4	-	2022-04-07 12:49:08	2022-04-07 12:49:08	编辑 删除
深圳	位置	2	-	2022-04-05 15:10:32	2022-04-05 15:10:32	编辑 删除
生产环境	环境	1	-	2022-04-05 15:10:23	2022-04-05 15:10:23	编辑 删除

标签管理可以设置不同类型的标签下，具体的标签信息。

- 1) 设置业务标签信息。业务标签一般指的是系统具体的业务内容，例如账户管理、用户信息、推荐系统等。
- 2) 设置环境标签信息。环境标签一般指的是工作环境、生产环境、操作系统等相关信息。



3) 设置位置标签。位置标签一般是由资产部署的地理位置或者归属的云和租户信息。

工作组

工作组 标签

① 标签用于工作组的相关属性标注，组标签分为三类：业务、环境、位置。可根据需要创建、修改或删除不同类型的标签。

业务标签数

环境标签数

位置标签数
3↑

新增标签

标签名称
abc

新增标签

标签名称

abc

位置poc

位置

0

-

2022-04-07 12:50:22

2022-04-07 12:50:22

编辑 | 删除

环境poc

环境

1

-

2022-04-07 12:50:01

2022-04-07 12:50:01

编辑 | 删除

业务poc

业务

4

-

2022-04-07 12:49:08

2022-04-07 12:49:08

编辑 | 删除

深圳

位置

2

-

2022-04-05 15:10:32

2022-04-05 15:10:32

编辑 | 删除

生产环境

环境

1

-

2022-04-05 15:10:23

2022-04-05 15:10:23

编辑 | 删除

新增标签

标签名称

标签类型

标签备注

业务

新增

删除

确定

取消



步骤三：负载管理

最近更新时间: 2023-02-10 16:09:03

工作负载

帮助文档

工作负载

角色标签

工作负载总量

5个

主机 2 容器 3

负载策略状态

放行状态负载

0个

主机 0 容器 0

告警状态负载

5个

主机 2 容器 3

阻断状态负载

0个

主机 0 容器 0

默认分组负载

0个

主机 0 容器 0

工作组

输入关键词查询

DEFAULT

南洋测试工作组

南洋测试组2

poc

testzhang

xx11

比邛

主机

全部Agent状态

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

主机名称/IP	角色标签	Agent状态	操作系统	隔离状态	更新时间	操作
微隔离测试3 109.244.105.187(外) 172.16.0....	-	在线	centos7.2x86_64	已初始化	2022-04-13 11:09:51	编辑 拉组 隔离

共 1 项

10条 / 页

1 / 1 页

工作负载是用来查看工作组负载的相信信息，并可以进行配置。

- 1) 查看和编辑工作负载的相关信息。可以设置资产的相关信息，包括标签、角色等。
- 2) 快速给工作复杂进行拉组。根据资产的相关信息，快速帮助资产进行分组。
- 3) 隔离。对被攻击的资产进行隔离，隔离有的资产仅可以访问安全后他，其他业务则断开。



步骤四：角色标签

最近更新时间: 2023-02-10 16:09:03

角色标签用来给不同的工作负载进行快速标记，从而帮助标记相同的资产进行统一管理和相关设置。

工作负载

帮助文档

工作负载

角色标签

新增标签

请输入角色名称进行检索

Q

刷新

标签名称	关联工作负载	标签描述	创建时间	更新时间	操作
主机	1	-	2022-04-07 18:51:02	2022-04-07 18:51:02	编辑 删除
容器	2	-	2022-04-07 18:50:55	2022-04-07 18:50:55	编辑 删除

共 2 项

10 条 / 页

1

/ 1 页



步骤五：安全策略

最近更新时间: 2023-02-10 16:09:03

查看安全策略信息

安全策略用来让用户看到所有的策略，并编辑和查看策略的相关信息。

安全策略管理

安全策略总量

4个

安全策略状态

已创建规则策略

2个

未创建规则策略

2个

已关联工作组策略

0个

未关联工作组策略

0个

新建策略

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

安全策略名称	关联规则数	作用工作组	隔离方式	备注	创建时间	更新时间	操作
zhangtest关联完所有...	0	南洋测试组2	阻断	-	2022-04-12 16:25:44	2022-04-13 10:38:38	编辑 删除
xxxx	1	DEFAULT	放行	-	2022-04-08 10:22:43	2022-04-08 10:22:43	编辑 删除
poc	0	poc	告警	-	2022-04-07 15:28:13	2022-04-07 15:28:13	编辑 删除
南洋测试组策略	1	南洋测试工作组	告警	-	2022-04-05 15:11:19	2022-04-06 15:33:51	编辑 删除

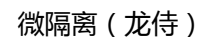
共 4 项

10 条 / 页

1 / 1 页

新建安全策略

新建安全需要填写以下信息。



×

* 策略名称 请输入策略名称，不超过32个字符

备注信息 请输入策略备注信息，不超过128个字符

★作用工作组 请选择策略生效的工作组

* 隔离方式  ☒ 放行 ☐ 告警 ☐ 阻断

方式一：通过异常访问记录创建

i 当策略生效的工作组为告警或拦截方式且未选择加白规则时，其他工作组的任意一次访问都被记录为异常，可根据实际需要，选择是否对其中的访问加白。

已加白的访问源 (0)

清空选择

近24小时

近7天

近30天

2022-04-27 ~ 2022-04-28



请输入访问源IP/工作组检索



访问源IP/工作组

访问次数

选择加白类型 

访问源IP/工作组	加白类型	时间

确认

取消

- 1) 基本信息。填写安全策略的名称。
- 2) 备注信息。填写安全策略的备注信息。
- 3) 工作组信息。填写安全策略的作用工作组，并设置如果和策略信息不符合，对应的操作。
- 4) 设置白名单信息。白名单信息有两种设置方法，一个是通过过往的访问记录添加，一个是用户手动输入。



步骤六：安全告警

最近更新时间: 2023-02-10 16:09:03

查看告警信息

如果有不符合安全策略的访问事件发生，则会出现安全告警。

告警列表

ⓘ 当被访问源工作组为告警或拦截方式且未选择对访问源加白处理时，任意一次访问都会被记录为告警；可根据需要，选择是否做加白处理。

近7天近14天近30天2022-04-21 ~ 2022-04-28📅

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

访问源IP/工作组	访问次数	被访问源IP/工作组	服务名称	协议/端口	隔离状态 ▾	告警发生时间	操作 ⓘ
暂无数据							

共 0 项

10 ▾ 条 / 页

⏮️⏪️1/1 页⏩️⏭️

/ngms/event/alertlist

处理告警信息

告警信息的处理方法有三种

- 1) 将来源加白。将访问来源设置为对应策略的白名单，后续不会产生告警。
- 2) 整组加白。如果访问来源有对应的工作组，可以将整组都设置为对应策略的白名单。
- 3) 单资产隔离。如果访问信息确实是由于访问源本身的问题，例如被漏洞利用或者已经是僵尸进程攻击的肉机，可以通过单资产隔离，从而减少攻击的影响

版权所有：建行云

第24 页 共25页



最佳实践

工作组

最近更新时间: 2023-02-10 09:55:28

对于分组，建议按最小集群进行分组。在新建工作组时，填写规范建议如下：

- 组名信息

名称：部署单元+加集群名称

备注：租户或者项目组根据实际情况填写

- 标签信息

业务：物理子系统名

环境：生产或测试

位置：北京或武汉

工作负载标签

建议按部署单元或者集群名称进行标记，以便拉组时可以方便筛选。

策略配置

- ☐ 策略名称：物理子系统+部署单元+集群名访问策略

- ☐ 备注：租户或者项目组根据实际需要填写

- ☐ 作用工作组：选择需要设置的工作组（工作组和策略为一对一关系）

- ☐ 隔离方式：选择告警模式（为避免业务影响阻断模式暂不开通）

- ☐ 白名单：建议按方式二先行添加，可按工作组模式直接选择，也可按ip或者ip段填写。但二者不能同时作用，所以如果有云外ip访问，建议按ip进行设置白名单。

对于安全事件

租户应随时关注，对于正常访问及时进行加白，对于异常访问及时进行处置。如遇真实负载沦陷场景，应及时通过一键隔离功能对风险负载进行隔离。

使用约束

- ☐ 一键隔离功能是通过调用主机或者容器内的iptables实现。所以对于容器建议大家全部安装iptables，以应对紧急情况。

- ☐ 目前仅支持Linux操作系统，暂不支持Windows。已适配主流的Linux内核，如遇不支持的可向建行数据中心安全团队反馈。